HINDI

VPN, LINUX FIREWALL AND PROXY SERVER BEGINNER PRACTICAL GUIDE

VPN, LINUX FIREWALL AND PROXY SERVER BEGINNER PRACTICAL GUIDE IN HINDI

www.cprogrammingbookinhindi.com

DIGITAL DOWNLOAD हिंदी

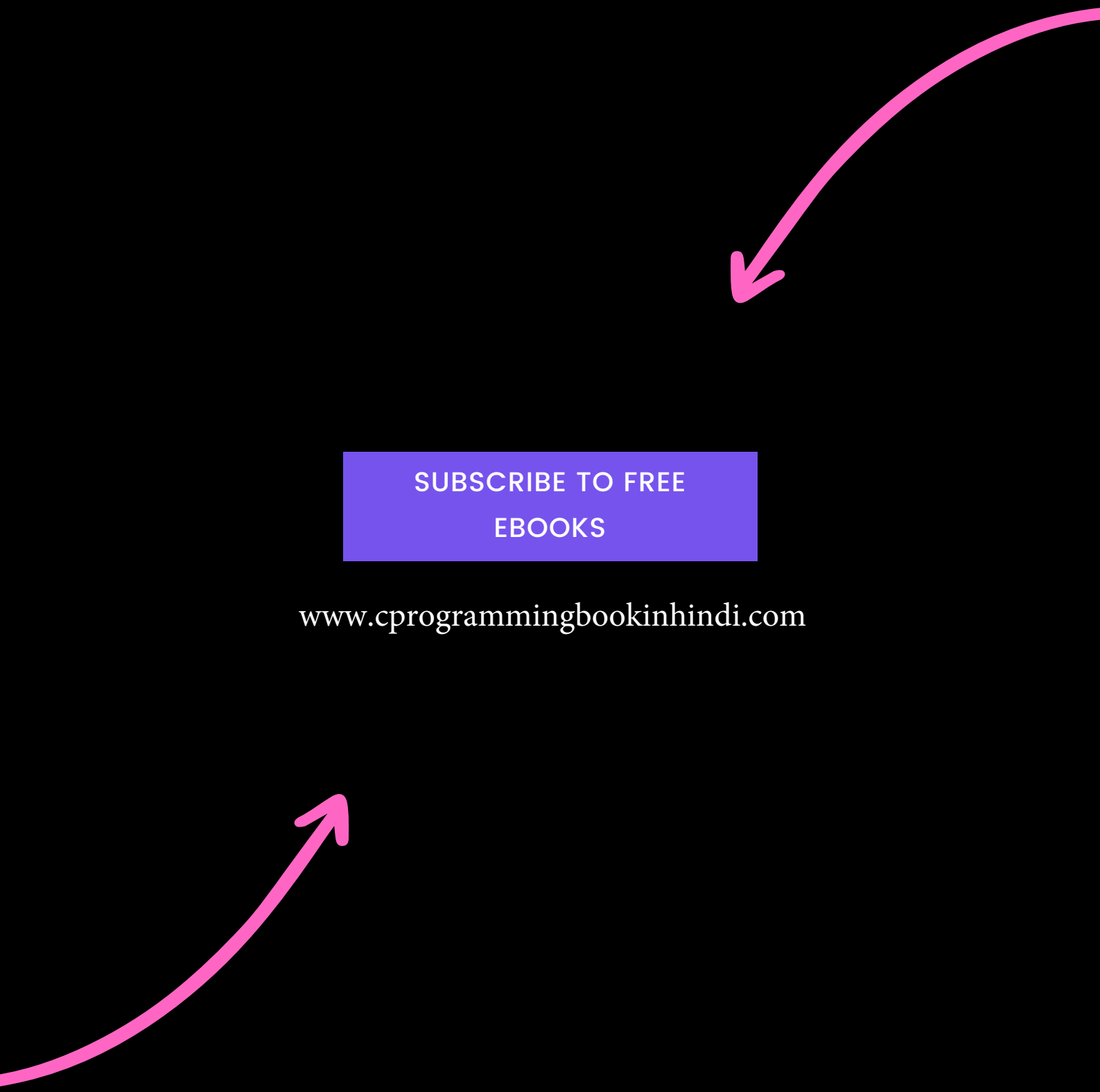
VPN, LINUX FIREWALL AND PROXY SERVER BEGINNER PRACTICAL GUIDE

Thanks for purchasing this Digital Download.

What's the success?

“We learn from failure, not from success!”
— Bram Stoker, Dracula

Please Keep this PDF in a safe place!


SUBSCRIBE TO FREE
EBOOKS
www.cprogrammingbookinhindi.com

VPN, LINUX FIREWALL AND PROXY SERVER BEGINNER PRACTICAL GUIDE IN HINDI

Copyright © 2017 by Machhindra Kalan

All rights reserved. No part of this work may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage or retrieval system, without the prior written permission of the copyright owner and the publisher.

Trademarked names may appear in this book. Rather than use a trademark symbol with every occurrence of a trademarked name, we use the names only in an editorial fashion and to the benefit of the trademark owner, with no intention of infringement of the trademark.

Lead Editor: Machhindra Kalan

Distributed to the book trade worldwide by Web Study Lab Pvt Ltd, Location - Mumbai, Palava city Pin 421204

E-mail: machhi29@gmail.com, or

Visit: www.cprogrammingbookinhindi.com

For information on translations, please contact Web Study Lab Pvt Ltd, Location - Mumbai, Palava city Pin 421204

Phone +91 86555-67778

The information in this book is distributed on an “as is” basis, without warranty. Although every precaution has been taken in the preparation of this work, the author shall not have any liability to any person or entity with respect to any loss or damage caused or alleged to be caused directly or indirectly by the information contained in this book.

This book
is dedicated
to those

who really wants
to be a

VPN, LINUX FIREWALL AND PROXY SERVER BEGINNER PRACTICAL GUIDE IN HINDI

INDEX OF CONTENTS

TABLE OF CONTENTS

Chapter 1: What is VPN 9
VPN Security

Chapter 2: Business Considerations……..12
VPN Deployment
Types of VPN product

Chapter 3: Common VPN Tunneling Technologies…….....25
IPsec (Internet Protocol Security)
PPTP (Point-to-Point Tunneling Protocol)
L2TP (Layer 2 Tunneling Protocol)
SSL / TLS

Chapter 4: Risks & Limitations of VPN……...29
Hacking Attacks
User Authentication
Client Side Risks
Virus / Malware Infections
Incorrect Network Access Rights
Interoperability

Chapter 5: Security Considerations 35
General VPN Security Considerations
Extranet VPN Security Considerations
Client Side VPN Security Considerations
Common Security Features in VPN Products

Conclusion ……...37

PART II

Chapter 6: Understanding Firewalls……38

Chapter 7: Firewall Architecture

Chapter 8: Setting up the Linux Filtering Firewall

Chapter 9: Software requirements

Chapter 10: Preparing the Linux system

Chapter 11: IP filtering setup (IPFWADM)

Chapter 12: IP filtering setup (IPCHAINS)

Chapter 13: Installing a Transparent SQUID proxy

Chapter 14: Installing the TIS Proxy server

Chapter 15: The SOCKS Proxy Server

Chapter 16: Advanced Configurations

Chapter 17: Making Management Easy

Chapter 18: Defeating a Proxy Firewall

INTRODUCTION

सुदूर स्थानों से आंतरिक नेटवर्क से जुड़ने के लिए आजकल मांग बढ़ रही है। कर्मचारियों को अक्सर घर, होटल, हवाई अड्डों या अन्य बाहरी नेटवर्क से इंटरनेट पर आंतरिक निजी नेटवर्क (जो कि प्रकृति असुरक्षित है) से जुड़ने की आवश्यकता होती है। जब कर्मचारी या व्यावसायिक भागीदार असुरक्षित बाहरी स्थानों से आंतरिक नेटवर्क तक निरंतर पहुंच रखते हैं, तो सुरक्षा एक प्रमुख विचार बन जाता है।

VPN (Virtual Private Network) प्रौद्योगिकी इंटरनेट पर प्रसारित होने वाली सूचनाओं की सुरक्षा करने का एक तरीका प्रदान करती है, जिससे उपयोगकर्ताओं को एक आंतरिक नेटवर्क में सुरक्षित रूप से एक असुरक्षित नेटवर्क के माध्यम से एक आंतरिक नेटवर्क में प्रवेश करने के लिए एक आभासी निजी "tunnel" स्थापित करने की अनुमति मिलती है। यह पेपर वीपीएन और कोर वीपीएन प्रौद्योगिकियों का एक सामान्य अवलोकन प्रदान करता है। हम संभावित सुरक्षा जोखिमों के साथ–साथ सुरक्षा विचारों पर भी चर्चा करते हैं जिन्हें वर्चुअल प्राइवेट नेटवर्क को लागू करते समय ध्यान में रखना चाहिए।

CHAPTER 1

WHAT IS VPN?

वीपीएन (वर्चुअल प्राइवेट नेटवर्क) एक सामान्य शब्द है जिसका उपयोग संचार नेटवर्क का वर्णन करने के लिए किया जाता है जो किसी भी असुरक्षित या अविश्वसनीय नेटवर्क 1 के माध्यम से कनेक्शन को सुरक्षित करने के लिए प्रौद्योगिकियों के किसी भी संयोजन का उपयोग करता है। एक समर्पित कनेक्शन का उपयोग करने के बजाय, जैसे कि लीज्ड लाइन, इंटरनेट जैसे किसी साझा या सार्वजनिक नेटवर्क पर भौगोलिक रूप से बिखरे हुए उपयोगकर्ताओं और नेटवर्क के बीच एक आभासी संबंध बनाया जाता है। डेटा को प्रेषित किया जाता है जैसे कि वह निजी कनेक्शन से गुजर रहा हो। वीपीएन tunnel के माध्यम से डेटा प्रसारित करता है। किसी पैकेट को प्रसारित करने से पहले, उसे एक नए हेडर के साथ एक नए पैकेट में लिपटे (लिपटे) किया जाता है। यह शीर्षलेख रूटिंग जानकारी प्रदान करता है ताकि यह एक साझा या सार्वजनिक नेटवर्क को पार कर सके, इससे पहले कि यह tunnel के समापन बिंदु तक पहुंच जाए। यह तार्किक पथ जो एन्कैप्सुलेटेड पैकेट से होकर जाता है उसे tunnel कहा जाता है।

जब प्रत्येक पैकेट tunnel के समापन बिंदु पर पहुंच जाता है, तो यह "विघटित" हो जाता है और अपने अंतिम गंतव्य को भेज दिया जाता है। दोनों tunnel समापन बिंदु को एक ही tunnel प्रोटोकॉल का समर्थन करने की आवश्यकता है। टनलिंग प्रोटोकॉल ओएसआई (ओपन सिस्टम इंटरकनेक्शन) लेयर दो (डेटा–लिंक लेयर), या लेयर थ्री (नेटवर्क लेयर) पर संचालित होते हैं। सबसे अधिक इस्तेमाल किया जाने वाला टनलिंग प्रोटोकॉल IPsec, L2TP, PPTP और SSL हैं। एक निजी गैर–निष्क्रिय आईपी पते के साथ एक पैकेट को विश्व स्तर पर अद्वितीय आईपी पते के साथ एक पैकेट के अंदर भेजा जा सकता है, जिससे इंटरनेट पर एक निजी नेटवर्क का विस्तार हो सकता है।

VPN SECURITY

वीपीएन डेटा गोपनीयता प्रदान करने के लिए एनक्रिप्शन का उपयोग करता है। एक बार कनेक्ट होने के बाद, वीपीएन एक सुरक्षित नेटवर्क में एनक्रिप्टेड डेटा को एनक्रिप्ट करने के लिए ऊपर वर्णित टनलिंग तंत्र का उपयोग करता है, खुले तौर पर पढ़ने वाले हेडर के साथ जो एक सार्वजनिक नेटवर्क को पार कर सकता है। इस तरह से एक सार्वजनिक नेटवर्क पर पारित पैकेट उचित डिक्रिप्शन कुंजी के बिना अपठनीय हैं, इस प्रकार यह सुनिश्चित करना कि डेटा का खुलासा नहीं किया गया है या ट्रांसमिशन के दौरान किसी भी तरह से बदल दिया गया है। वीपीएन एक डेटा अखंडता जांच भी प्रदान कर सकता है। यह आमतौर पर यह सुनिश्चित करने के लिए एक संदेश डाइजेस्ट का उपयोग करके किया जाता है कि ट्रांसमिशन के दौरान डेटा के साथ छेड़छाड़ नहीं की गई है। डिफ़ॉल्ट रूप से, वीपीएन मजबूत उपयोगकर्ता प्रमाणीकरण प्रदान या लागू नहीं करता है। उपयोगकर्ता घर से या अन्य असुरक्षित नेटवर्क के माध्यम से एक आंतरिक निजी नेटवर्क तक पहुंच प्राप्त करने के लिए एक साधारण उपयोगकर्ता नाम और पासवर्ड दर्ज कर सकते हैं। फिर भी, वीपीएन ऐड–ऑन ऑथेंटिकेशन मेकेनिज्म, जैसे स्मार्ट कार्ड, टोकन और RADIUS का समर्थन करता है।

CHAPTER 2

BUSINESS CONSIDERATIOS

VPN DEPLOYMENT

वीपीएन मुख्य रूप से संगठनों और उद्यमों द्वारा निम्नलिखित तरीकों से नियोजित किया जाता है:

1- Remote एक्सेस वीपीएन: यह घर के लिए एक उपयोगकर्ता–से–नेटवर्क कनेक्शन है, जो एक मोबाइल उपयोगकर्ता को ऑरमोट स्थान से कॉर्पोरेट निजी नेटवर्क से कनेक्ट करने की इच्छा रखते हैं। इस तरह के वीपीएन एक कॉर्पोरेट निजी नेटवर्क और दूरस्थ उपयोगकर्ताओं को सुरक्षित, एनक्रिप्टेड कनेक्शनबेट की अनुमति देता है।

2- इंटरनेट वीपीएन: यहां, वीपीएन का उपयोग शाखा कार्यालयों के रूप में निश्चित स्थानों के बीच संबंध बनाने के लिए किया जाता है। इस प्रकार का LAN–to–LAN VPN कनेक्शन दूरस्थ स्थानों को एक ही निजी नेटवर्क में जोड़ता है।

3- एक्स्ट्रानेट वीपीएन: यह वह जगह है जहां वीपीएन का उपयोग व्यापारिक साझेदारों, सुक्स आपूर्तिकर्ताओं और ग्राहकों को जोड़ने के लिए किया जाता है, ताकि विभिन्न पक्षों को साझा वातावरण में डेटा को काम करने की अनुमति मिल सके।

4- WAN प्रतिस्थापन: जहां वीपीएन WAN (वाइड एरिया नेटवर्क) के लिए एक विकल्प प्रदान करता है। WAN का रखरखाव महंगा हो सकता है, खासकर जब नेटवर्क भौगोलिक रूप से छितरी हुई हो। वीपीएन को अक्सर कम लागत और ओवरडायलेशन ओवरहेड की आवश्यकता होती है, और पट्टे की रेखाओं का उपयोग करके पारंपरिक निजी नेटवर्क की तुलना में अधिक मापनीयता प्रदान करता है। हालांकि, नेटवर्क की विश्वसनीयता और प्रदर्शन की समस्या एक समस्या है, विशेष रूप से जब डेटा और कनेक्शन इंटरनेट पर टनलब्युलथ्रू हैं।

TYPES OF VPN PRODUCT

वीपीएन को मोटे तौर पर निम्नानुसार वर्गीकृत किया जा सकता है:

1- एक फ़ायरवॉल–आधारित वीपीएन एक है जो फ़ायरवॉल और वीपीएन दोनों क्षमताओं से लैस है। इस प्रकार का वीपीएन एक आंतरिक नेटवर्क तक पहुंच को प्रतिबंधित करने के लिए सुरक्षा तंत्र का उपयोग करता है। सुविधाएँ यह पता अनुवाद, उपयोगकर्ता प्रमाणीकरण, वास्तविक समय अलार्म और प्रसारण प्रदान करता है।

2- एक हार्डवेयर–आधारित वीपीएन उच्च नेटवर्क थ्रूपुट, बेहतर प्रदर्शन और themore विश्वसनीयता प्रदान करता है, क्योंकि कोई प्रोसेसर ओवरहेड नहीं है। हालाँकि, यह अधिक सस्ती भी है।

3- एक सॉफ़्टवेयर–आधारित VPN ट्रैफ़िक प्रबंधित करने में सबसे अधिक लचीलापन प्रदान करता है।यह प्रकार उपयुक्त है जब वीपीएन एंडपॉइंट एक ही पार्टी द्वारा नियंत्रित नहीं किए जाते हैं, और जहां विभिन्न फायरवॉल और राउटर का उपयोग किया जाता है। इसका उपयोग प्रदर्शन बढ़ाने के लिए हार्डवेयर–एनक्रिप्शन त्वरक के साथ किया जा सकता है।

4- एक एसएसएल वीपीएन उपयोगकर्ताओं को एक वेब ब्राउज़र का उपयोग करके वीपीएन उपकरणों से कनेक्ट करने की अनुमति देता है।एसएसएल (सिक्योर सॉकेट्स लेयर) प्रोटोकॉल या टीएलएस (ट्रांसपोर्ट लेयर सिक्योरिटी) प्रोटोकॉल का उपयोग वेब ब्राउजर और एसएसएल वीपीएनदेवस के बीच ट्रैफिक को एनक्रिप्ट करने के लिए किया जाता है। एसएसएल वीपीएन का उपयोग करने का एक फायदा उपयोग में आसानी है, क्योंकि सभी स्टैंडर्डव्यू ब्राउज़र एसएसएल प्रोटोकॉल का समर्थन करते हैं, इसलिए उपयोगकर्ताओं को किसी भी इंस्टॉलेशन या कॉनफ़िगरेशन को करने की आवश्यकता नहीं है।

CHAPTER 3

COMMON VPN TUNNELING TECHNOLOGIES

वीपीएन में आमतौर पर निम्नलिखित टनलिंग तकनीकों का उपयोग किया जाता है:

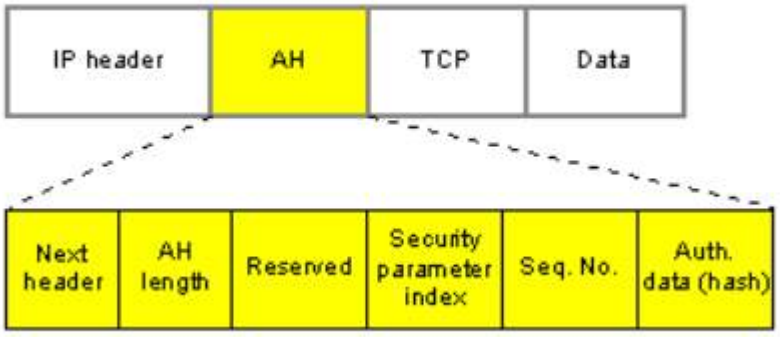
IPSEC (इंटरनेट परियोजना सुरक्षा))

IPsec का विकास IETF (इंटरनेट इंजीनियरिंग टास्क फोर्स) द्वारा किया गया था, जो इंटरनेट के रूप में सार्वजनिक असुरक्षित आईपी नेटवर्क पर OSI परत तीन में सूचना के सुरक्षित हस्तांतरण के लिए किया गया था। IPsec आवश्यक सुरक्षा प्रोटोकॉल, एल्गोरिथम (ओं) और गुप्त कुंजियों के चयन के लिए एक प्रणाली को सक्षम करता है जो अनुरोध की गई सेवाओं के लिए उपयोग की जाती हैं। IPsec डेटा के अनधिकृत देखने और संशोधन की सुरक्षा के लिए बुनियादी प्रमाणीकरण, डेटा अखंडता और एनक्रिप्शन सेवाएं प्रदान करता है। यह आवश्यक सेवाओं के लिए दो सुरक्षा प्रोटोकॉल, एएच (प्रमाणीकरण हेडर) और ईएसपी (एनकैप्सुलेटेड सिक्योरिटी पेलोड) का उपयोग करता है। हालाँकि, IPsec केवल IP पैकेट भेजने तक सीमित है।

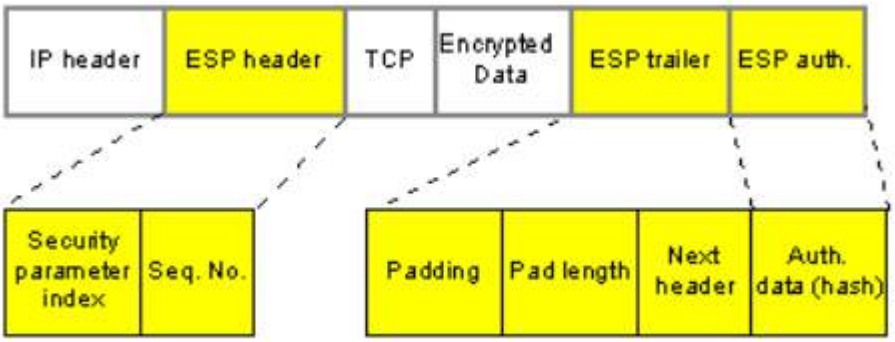
यातायात सुरक्षा के लिए सुरक्षा प्रोटोकॉल

IPsec सुरक्षा सेवाओं को प्रदान करने के लिए AH और ESP प्रोटोकॉल का उपयोग करता है:

1- AH (ऑथेंटिकेशन हैडर) प्रोटोकॉल IP पैकेट्स के सोर्स ऑथेंटिकेशन और इनइन्ग्रेटिटी प्रदान करता है, लेकिन इसमें एनक्रिप्शन नहीं है। आईपी पैकेट में एक एएच हेडर जोड़ा गया है जिसमें डेटा का एक हैश, एक अनुक्रम संख्या आदि है, और सूचना को प्रेषक को सत्यापित करने के लिए इस्तेमाल किया जा सकता है, जो डेटा अखंडता सुनिश्चित करता है और फिर से खेलना हमलों को नियंत्रित करता है।



2- ESP (एनकैप्सुलेटेड सिक्योरिटी पेलोड) प्रोटोकॉल डेटा की गोपनीयता प्रदान करता है। ईएसपी डेटा गोपनीयता प्रदान करने के लिए 3 डीईएस जैसे सममिति एल्गोरिदम एल्गोरिदम का उपयोग करता है। एल्गोरिथम दोनों संचार करने वाले साथियों पर एक जैसा होता है। ESP केवल–समर्थन या प्रमाणीकरण–केवल कॉनफ़िगरेशन का भी समर्थन कर सकता है। हालाँकि, in2007 के अनुसंधान से पता चला कि IPsec का कोई भी RFC– आज्ञाकारी कार्यान्वयन जो एनक्रिप्शन–केवल ESP का उपयोग करता है, को तोड़ा जा सकता है।



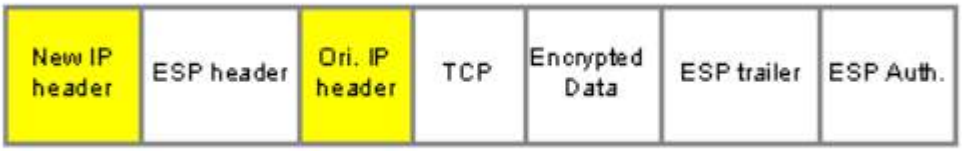
3-

MODES OF OPERATION

प्रत्येक सुरक्षा प्रोटोकॉल ऑपरेशन के दो तरीकों का समर्थन करता है: एक tunnel मोड और एक परिवहन मोड। टनल मोड एनक्रिप्ट और / या हेडर और प्रत्येक पैकेट के डेटा को प्रमाणित करता है जबकि ट्रांसपोर्ट मोड केवल एनक्रिप्ट और / या डेटा को ही प्रमाणित करता है।

1- टनल मोड (एंड–टू–एंड)

यहां पूरा पैकेट सुरक्षित है। मूल आईपी पैकेट, मूल पते के साथ, एक नए आईपी पैकेट में डाला जाता है और एएच और ईएसपी नए पैकेट के लिए लागू होता है। नया IP हेडर thetunnel के अंतिम बिंदु की ओर इशारा करता है। पैकेट की प्राप्ति के बाद, टनल एंड पॉइंट कॉनसेंट को डिक्रिप्ट करेगा और मूल पैकेट को आगे चलकर अपने अंतिम गंतव्य Ingetget नेटवर्क पर भेजा जाएगा।



2- ट्रांसपोर्ट मोड (होस्ट–टू–होस्ट)

यहां एएच और ईएसपी हेडर को मूल आईपीपैकेट के डेटा पर लागू किया जाता है। मोड एनक्रिप्ट करता है और / या डेटा को प्रमाणित करता है लेकिन IPheader नहीं। जोड़ा गया ओवरहेड tunnel मोड में आवश्यक से कम है।हालाँकि, अंतिम गंतव्य और स्रोत पते सूँघे जा सकते हैं।हमलावर हेडर की थीस्टाइप में हेडर सूचना के आधार पर ट्रैफ़िक विश्लेषण कर सकते हैं। यह आमतौर पर केवल होस्ट–टू–होस्ट कनेक्शन के लिए उपयोग किया जाता है।

Key Exchange and Management

IPsec इंटरनेट पर दो प्रकार के प्रमुख प्रबंधन का समर्थन करता है: स्वचालित और मैनुअल।

1- Automated Key Management

IKE (इंटरनेट कुंजी विनिमय) IPsec todetermine और वार्ता प्रोटोकॉल, एल्गोरिदम और कुंजियों का उपयोग करने और प्रमाणित करने के लिए डिफ़ॉल्ट प्रोटोकॉल है।

दो दलों। यह वीपीएन के व्यापक, स्केलेबल परिनियोजन और कार्यान्वयन के लिए उपयोगी है। IKEv2 प्रोटोकॉल में जारी किया गया था 2005. यह IKEv1 प्रोटोकॉल की अधिकांश कार्यक्षमता को संरक्षित करता है, लेकिन नेटवर्क एड्रेस ट्रांसलेशन (NAT) ट्रैवर्सल का भी समर्थन करता है और अधिक लचीलापन प्रदान करता है।

IKE भी डिजिटल प्रमाणपत्र के उपयोग का समर्थन करता है। उपयोगकर्ता पहले अपने डिजिटल हस्ताक्षर कुंजी के साथ डेटा पर हस्ताक्षर करके प्रमाणित करते हैं। अन्य समापन बिंदु फिर हस्ताक्षर को सत्यापित करेगा। IKE दो संस्थाओं के बीच एक प्रमाणित, सुरक्षित tunnel बनाता है, फिर दो संस्थाओं के बीच एक सुरक्षा संघ (SA), और कुंजी (ओं) का आदान–प्रदान करता है। एसए यातायात की सुरक्षा के लिए सेवाओं और तंत्र को परिभाषित करने के लिए साथियों से बातचीत करके उपयोग किए जाने वाले मापदंडों

का एक समूह है। इन मापदंडों में एल्गोरिथ्म आइडेंटिफ़ायर, मोड्स, कीज़ आदि शामिल हैं। IKE भी चाबियों का ट्रैक रखता है और संवाद करने वाले साथियों के बीच उन्हें अपडेट करता है। IKE, ISAKMP (इंटरनेट सिक्योरिटी एसोसिएशन और की मैनेजमेंट प्रोटोकॉल) और ओकली जैसे प्रोटोकॉल का उपयोग करता है, जो कि प्रमुख पीढ़ी, निर्माण और SA और प्रमाणीकरण के प्रबंधन के लिए प्रक्रियाओं को परिभाषित करता है।

कई प्रमाणीकरण विधियां हैं जो एक IPsec वीपीएन गेटवे दूरस्थ उपयोगकर्ता प्रमाणीकरण 5 के लिए IKE के साथ काम करता है, जिसमें हाइब्रिड प्रमाणीकरण, eXtended प्रमाणीकरण (Xauth), क्रिप्टोग्राफिक कुंजी (CRACK), और डिजिटल प्रमाणपत्र के लिए चुनौती / प्रतिक्रिया प्रमाणीकरण शामिल हैं। यह एक्सेस कंट्रोल प्रक्रिया को मजबूत करने के लिए अतिरिक्त तृतीय–पक्ष प्रमाणीकरण सेवाओं का उपयोग करने की अनुमति देता है।

2- Manual key management

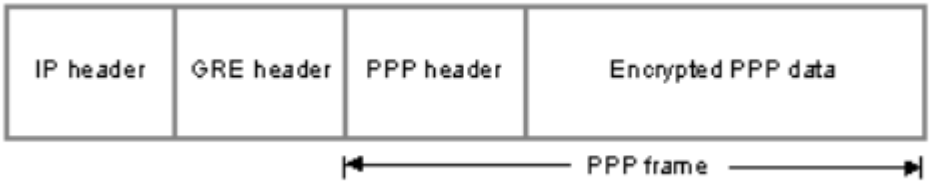
गुप्त कुंजी (Secret keys) और सुरक्षा संघ मैन्युअल रूप से एक कनेक्शन शुरू होने से पहले दोनों VPN संवाद स्थापित साथियों में कॉनफ़िगर किए गए हैं। केवल प्रेषक और प्राप्तकर्ता हाथ में सुरक्षा सेवाओं के लिए गुप्त कुंजी जानता है। यदि थ्रेडहेंटिकेशन डेटा मान्य है, तो प्राप्तकर्ता जानता है कि संचार

प्रेषक से आया था और इसे संशोधित नहीं किया गया था। यह दृष्टिकोण छोटे, स्थिर वातावरण में उपयोग करना आसान है, लेकिन यह अच्छी तरह से पैमाने पर नहीं है। सभी कुंजी को पहले से सुरक्षित रूप से साथियों को संप्रेषित करने के लिए वितरित किया जाना चाहिए। यदि कुंजियों से छेड़छाड़ की जाती है, तो दूसरा व्यक्ति उपयोगकर्ता के रूप में मुद्रा बना सकता है और वीपीएन में संबंध बना सकता है।

पीपीटीपी (**POINT–TO–POINT TUNNELING PROTOCOL**)

PPTP (पॉइंट–टू–पॉइंट टनलिंग प्रोटोकॉल) एक OSI लेयर दो प्रोटोकॉल है जो PPP (पॉइंट–टू–पॉइंट प्रोटोकॉल) के ऊपर बनाया गया है। पीपीपी एक बहु–प्रोटोकॉल, डायल–अप प्रोटोकॉल है जिसका उपयोग इंटरनेट से जुड़ने के लिए किया जाता है। दूरस्थ उपयोगकर्ता अपने स्थानीय ISP में पहली बार डायल करके PPTP के माध्यम से एक निजी नेटवर्क का उपयोग कर सकते हैं। PPTP प्रत्येक दूरस्थ क्लाइंट के लिए वर्चुअल नेटवर्क बनाकर लक्ष्य नेटवर्क से जुड़ता है। पीपीटीपी गैर–टीसीपी / आईपी प्रोटोकॉल (जैसे आईपी, आईपीएक्स या नेटबीयूआई) के साथ पीपीपी सत्र की अनुमति देता है, जिसे आईपी नेटवर्क के माध्यम से ट्यून किया जा सकता है। पीपीटीपी को आरएफसी 2637 में सूचना के मसौदे के रूप में प्रलेखित किया गया है।

PPP कनेक्शन के लिए उपयोग किया जाने वाला समान प्रमाणीकरण तंत्र PPTP– आधारित वीपीएन कनेक्शन में समर्थित है। इनमें EAP (एक्स्टेंसिबल ऑथेंटिकेशन प्रोटोकॉल, MS–CHAP (Microsoft चैलेंज–हैंडशेक ऑथेंटिकेशन प्रोटोकॉल), CHAP, SPAP (शिवा पासवर्ड ऑथेंटिकेशन प्रोटोकॉल) और PAP (पासवर्ड ऑथेंटिकेशन प्रोटोकॉल) शामिल हैं। एनक्रिप्शन के लिए, PPP डेटा को वैकल्पिक रूप से MPPE (Microsoft पॉइंट–टू–पॉइंट एनक्रिप्शन) का उपयोग करके एनक्रिप्ट किया जा सकता है जो लिंक एनक्रिप्शन के लिए RSA RC4 (40 / 56 / 128 बिट) मानक पर आधारित है।



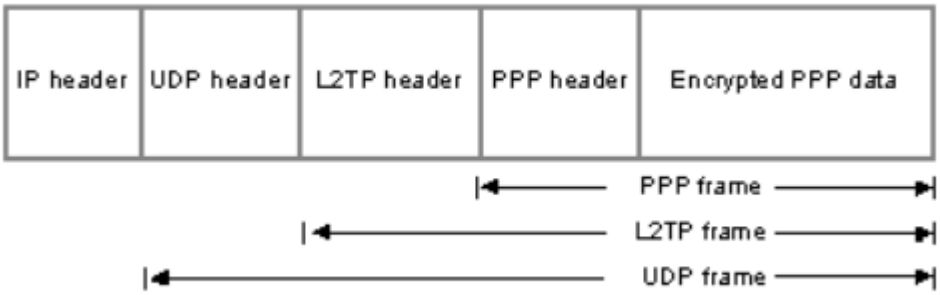
PPTP डेटा टनलिंग, एनकैप्सुलेशन के कई स्तरों के माध्यम से पूरा किया जाता है। PPTP IP नेटवर्क पर ट्रांसमिशन के लिए ट्यून किए गए डेटा के रूप में PPP फ्रेम को एनकैप्सुलेट करता है, जैसे कि

जीआरई (जेनेरिक रूटिंग इनकैप्सुलेशन) के संशोधित संस्करण का उपयोग करके इंटरनेट या एक निजी इंट्रानेट। GRE PPP पैकेट ले जाने के लिए एक प्रवाह और भीड़ नियंत्रित नियंत्रित सेवा प्रदान करता है। एन्कैप्सुलेटेड पीपीपी फ्रेम में डेटा एनक्रिप्ट किया जा सकता है (और / या संपीड़ित)। परिणामी GRE–&–PPP– एनकैप्सुलेटेड डेटा को तब PPTP क्लाइंट और PPTP सर्वर के लिए उपयुक्त स्रोत और गंतव्य IP पतों वाले IP हेडर के साथ समझाया जाता है। PPTP ट्यून किए गए डेटा की प्राप्ति पर, PPTP सर्वर प्रोसेस करता है और IP, GRE और PPP हेडर को निकालता है, फिर PPP डेटा को डिक्रिप्ट (और / या डिकम्प्रेस) करता है।

L2TP (LAYER 2 TUNNELING PROTOCOL)

L2TP (लेयर 2 टनलिंग प्रोटोकॉल) Microsoft PPTP (पॉइंट–टू–पॉइंट टनलिंग प्रोटोकॉल) और सिस्को L2F (लेयर 2 फॉरवर्डिंग) का एक संयोजन है। L2TP को IP, X पर भेजे जाने वाले PPP (पॉइंट–टू–पॉइंट प्रोटोकॉल) फ्रेम को एनकैप्सुलेट करने के लिए एक टनलिंग प्रोटोकॉल के रूप में उपयोग किया जा सकता है।25, फ़्रेम रिले या एटीएम नेटवर्क। एक tunnel के माध्यम से कई कनेक्शनों की अनुमति है। PPTP और L2F की तरह, L2TP OSI लेयर दो पर काम करता है। दो वीपीएन प्रोटोकॉल लेयर पीपीपी फ्रेम में डेटा को एनकैप्सुलेट करते हैं और एक आईपी नेटवर्क पर गैर–आईपी प्रोटोकॉल प्रसारित करने में सक्षम होते हैं। L2TP मानक ट्रैक के रूप में RFC 3931 में प्रलेखित है। L2TP कनेक्शन PPP कनेक्शन, जैसे कि EAP, CHAP, MS–CHAP, PAP और SPAP के समान प्रमाणीकरण तंत्र का उपयोग करते हैं। L2TP टनलिंग एन्कैप्सुलेशन के कई स्तरों के माध्यम से पूरा किया जाता है। PPP डेटा पीपीपी हेडर और L2TP हेडर के भीतर एनकैप्सुलेटेड है। L2TP एन्कैप्सुलेटेड पैकेट को स्रोत और गंतव्य पोर्ट

के साथ सेट किए गए UDP हेडर में लपेटा जाता है1701. अंतिम पैकेट एक आईपी हैडर के साथ वीपीएन क्लाइंट और वीपीएन सर्वर के स्रोत और गंतव्य आईपी पते युक्त होता है।



L2TP द्वारा प्रदान की गई गोपनीयता की कमी के कारण, इसे अक्सर IPsec के साथ संयोजन में उपयोग किया जाता है और L2TP / IPsec के रूप में संदर्भित किया जाता है। जब L2TP IPsec पर चल रहा है, तो IPsec, AH और ESP द्वारा सुरक्षा सेवाएँ प्रदान की जाती हैं। सभी L2TP नियंत्रण और डेटा IPsec सिस्टम में सजातीय आईपी डेटा पैकेट के रूप में दिखाई देते हैं।

एसएसएल / टीएलएस

एसएसएल / टीएलएस एक ट्रांसपोर्ट–लेयर प्रोटोकॉल है जो टीसीपी पोर्ट 443 का उपयोग करता है. एसएसएल प्रोटोकॉल आईईटीएफ द्वारा परिभाषित किया गया है और एसएसएल 3.1 संस्करण से परे कोई संस्करण नहीं हैं। टीएलएस1.0 और टीएलएस1.1 टीएलएस और टीएलएस के दो मानकीकृत संस्करण हैं1.0 एसएसएल के समान है3. 1।

एसएसएल / टीएलएस द्वारा प्रदान की जाने वाली कई क्रिप्टोग्राफिक विशेषताएं हैं और इनमें गोपनीयता, अखंडता और डिजिटल हस्ताक्षर शामिल हैं। IPsec के विपरीत, जिसमें दो संचार पक्ष क्रिप्टोग्राफ़िक

कार्यों के लिए सहमत होते हैं, SSL / TLS संचार करते समय उपयोग करने के लिए क्लाइंट और सर्वर के लिए क्रिप्टोग्राफ़िक फ़ंक्शंस के सेट को परिभाषित करने के लिए सिफर स्वीट्स का उपयोग करता है।

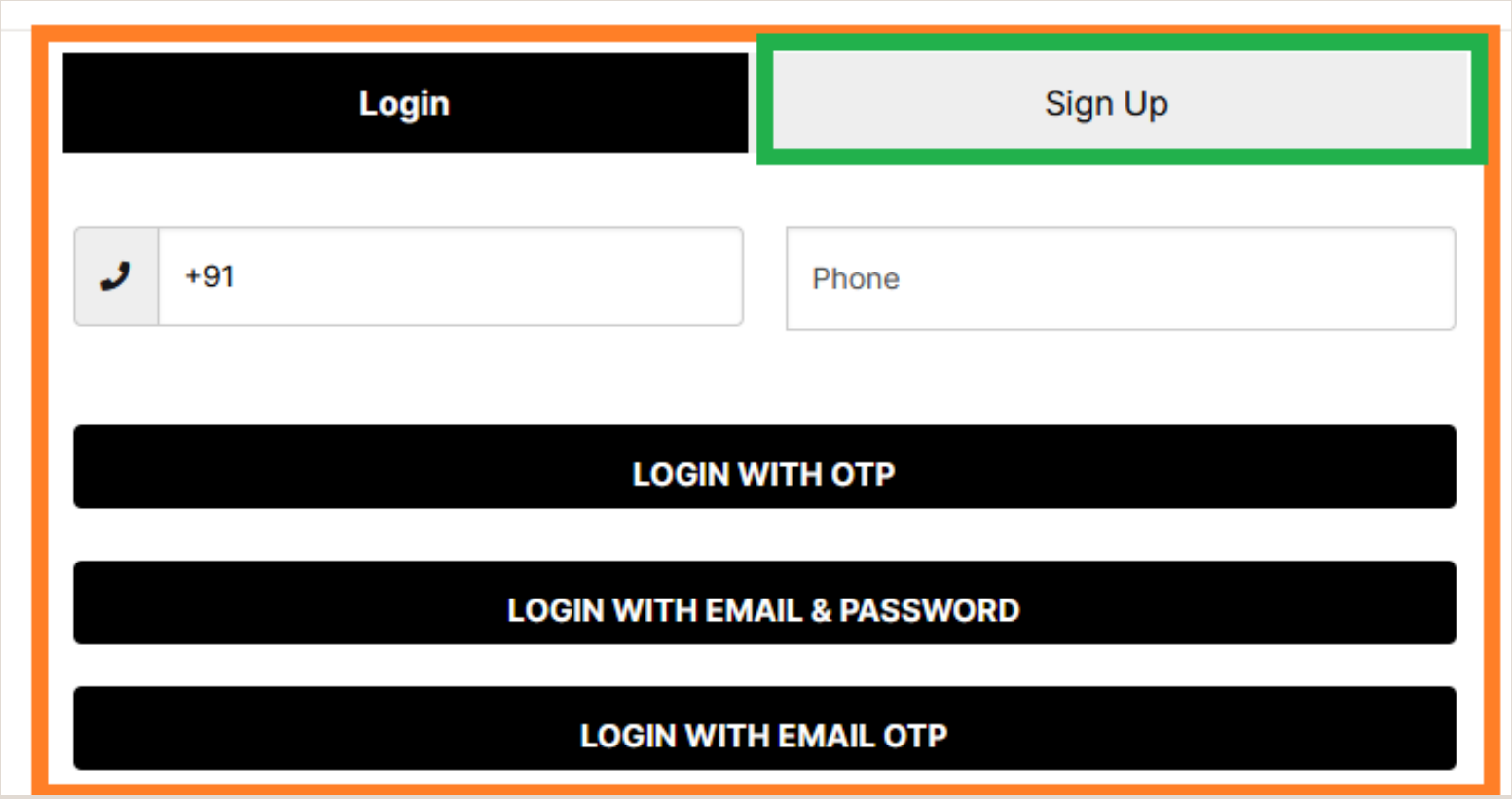
एक एसएसएल वीपीएन प्रवेश द्वार एक विश्वसनीय सीए (प्रमाणन प्राधिकरण) द्वारा हस्ताक्षरित एसएसएल सर्वर प्रमाणपत्र का उपयोग करके वेब उपयोगकर्ता को प्रमाणित कर सकता है, ताकि उपयोगकर्ता यह सत्यापित कर सके कि वह अपने ब्राउज़र के माध्यम से विश्वसनीय सर्वर से बात कर रहा है। व्यवहार में, कुछ एसएसएल वीपीएन एक स्व–हस्ताक्षरित डिजिटल प्रमाणपत्र का उपयोग कर सकते हैं जो आमतौर पर अधिकांश वेब ब्राउज़रों पर भरोसा नहीं किया जाता है। इस मामले में, उपयोगकर्ता को उपयोगकर्ता की विश्वसनीय सूची की एसएसएल वीपीएन सर्वर सर्टिफिकेट को जोड़ने या „हां स्वीकार करने की आवश्यकता हो सकती है। प्रमाण पत्र पर भरोसा करने के लिए।

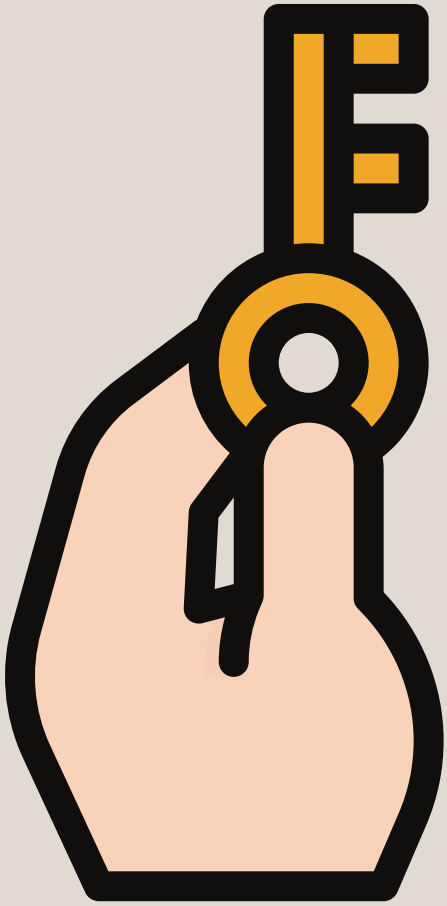
HOW TO GET COMPLETE PDF EBOOK

Pay Paytm

कोई भी **2 Ebooks** खरीदने पर **20%** डिस्काउंट- **India20**

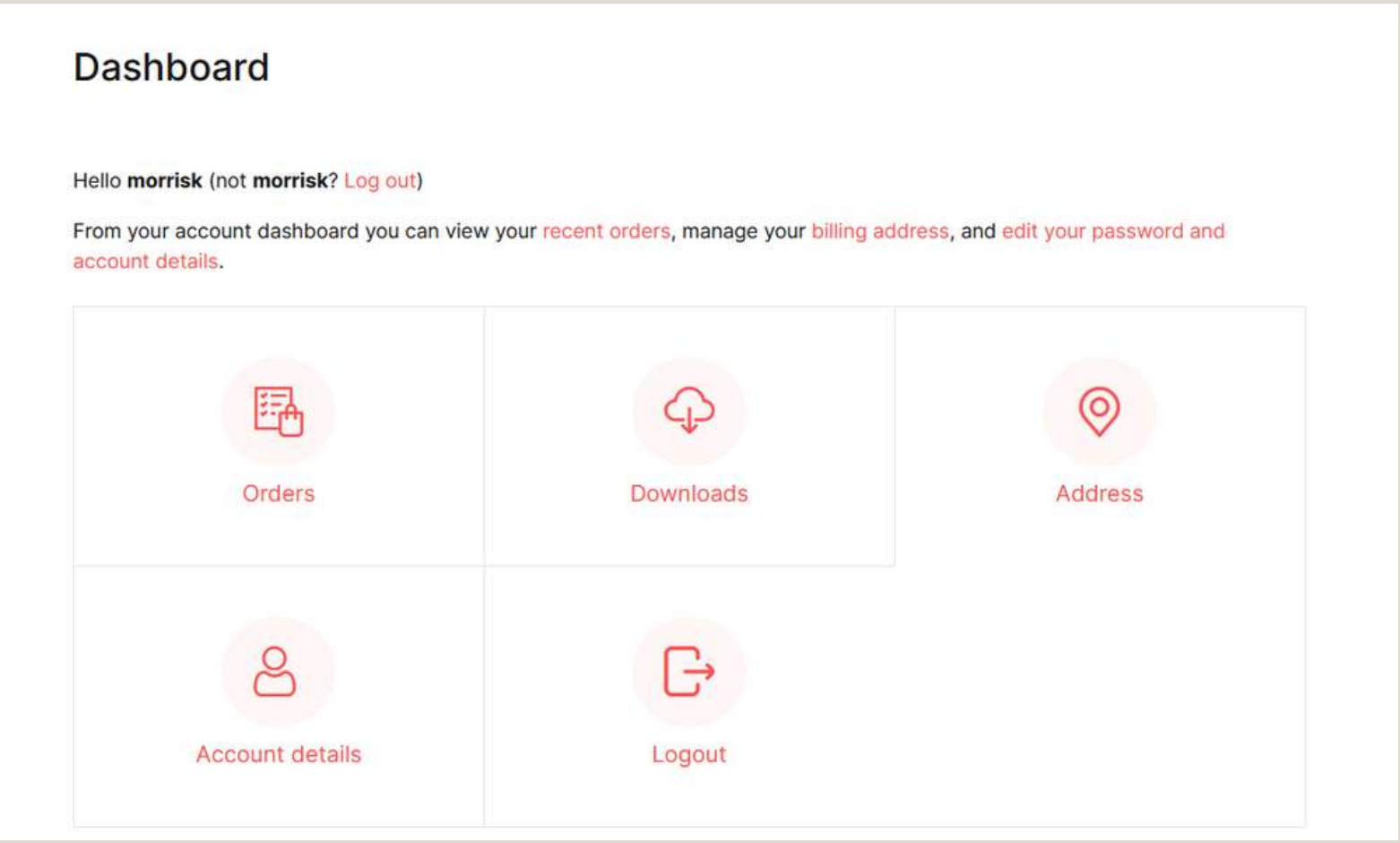
Buy Now पर क्लिक करने पर आपको **चेकआउट पेज** पर लॉगिन फॉर्म पर पहिले ईमेल से लॉगिन करना होगा।





Login Succesfull के बाद आपको पेमेंट करके Ebooks वही से डाउनलोड कर सकते है।

उसके बाद आप **My Account** पेज पर जाकर **Download** में Ebooks डाउनलोड कर सकते है।



Thank you